

"Express Mail" Label No.: EL 848970496 US

Date of Deposit: October 29, 2003

Attorney Docket No.14897US02

SECURITY SYSTEM FOR COMMUNICATING DATA
BETWEEN A MOBILE HANDSET AND A MANAGEMENT SERVER

RELATED APPLICATIONS

[0001] This patent application makes reference to, claims priority to and claims benefit from United States Provisional Patent Application Serial No. 60/422,048, entitled "Security System for Communicating Data between a Mobile Handset and a Management Sever," filed on October 29, 2002.

[0002] The complete subject matter of the above-referenced United States Patent Application is hereby incorporated herein by reference, in its entirety. In addition, this application makes reference to United States Provisional Patent Application Serial No. 60/249,606, entitled "System and Method for Updating and Distributing Information", filed November 17, 2000, and International Patent Application Publication No. WO 02/41147 A1, entitled "Systems And Methods For Updating And Distributing Information," publication date March 23, 2002, the complete subject matter of each of which is hereby incorporated herein by reference, in its entirety.

FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

[0003] [Not Applicable]

[MICROFICHE/COPYRIGHT REFERENCE]

[0004] [Not Applicable]

BACKGROUND OF THE INVENTION

[0005] The present invention relates generally to security of communications, and more specifically, the security of data communications, such as update packages for software and firmware, between a mobile handset and a management server.

[0006] Electronic devices, such as mobile phones and personal digital assistants (PDA's), often contain firmware and application software that are either provided by the manufacturers

of the electronic devices, by telecommunication carriers, or by third parties. These firmware and application software often contain software bugs. New versions of the firmware and software are periodically released to fix the bugs or to introduce new features, or both. Problems may arise when communicating data such as firmware/software updates between mobile electronic devices and the management servers that provide such data.

[0007] Security of mobile handsets has been handled, to some extent, by embedded security solutions employing security features built into a handset device. Cryptographic techniques have sometimes been employed to encrypt and decrypt data. Device authorization in mobile devices is one issue, and cryptographic protection is another issue in mobile device security. Device keys may be sometimes employed to provide for device authentication.

[0008] Further limitations and disadvantages of conventional and traditional approaches will become apparent to one of ordinary skill in the art through comparison of such systems with the present invention.

BRIEF SUMMARY OF THE INVENTION

[0009] Aspects of the present invention may be seen in a system that supports secure communication of data between an electronic device and a network, the system comprising the electronic device and the network. The electronic device comprising a first component that manages information in the electronic device; and a second component that provides access to proprietary information in the electronic device. At least one server manages the information communicated to the electronic device via the network. A first portion of information and a second portion of information is used to securely communicate data to the electronic device, the first portion of information and the second portion of information being managed by the at least one server and the first component to provide secure communication between the electronic device and the network.

[0010] In an embodiment of the present invention, the first portion of information comprises a first key and the second portion of information comprises a second key. In an embodiment of the present invention, the first key and the second key are combined to provide a higher level of security in the system and the data communication between the electronic device and the network relative to using the first key and the second key separately.

[0011] The method for securely communicating data and information in the system of the present invention, between an electronic device and a network, comprising storing a first security key; receiving a message containing a second security key; processing the received message; retrieving the second security key from the processed message; and generating a third security key.

[0012] In an embodiment of the present invention, the electronic device combines the first security key and the second security key to generate the third security key. The method further comprises employing the third security key for communication with the at least one server.

[0013] These and other features and advantages of the present invention may be appreciated from a review of the following detailed description of the present invention, along with the accompanying figures in which like reference numerals refer to like parts throughout.

BRIEF DESCRIPTION OF SEVERAL VIEWS OF THE DRAWINGS

[0014] Fig. 1A illustrates a block diagram of an exemplary security system for communicating data between a mobile handset and a management server, in accordance with an embodiment of the present invention.

[0015] Fig. 1B illustrates a block diagram of an exemplary security system 155 for communicating data between a mobile handset and a management server, in accordance with an embodiment of the present invention.

[0016] Fig. 2 illustrates a block diagram of an exemplary mobile handset employing a management client to manage secure communications of data/code with external systems, in accordance with an embodiment of the present invention.

[0017] Fig. 3 illustrates a flow diagram of an exemplary method of operating a secure system for communicating data between a mobile handset and a management server, in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0018] Fig. 1A illustrates a block diagram of an exemplary security system 105 for communicating data between a mobile handset and a management server, in accordance with an embodiment of the present invention. The security system 105 may facilitate secure communication of data/code between a mobile handset 107 and a carrier network 117. The carrier network 117 may employ a combination of at least a piece of information dynamically sent to the mobile handset 107 by the carrier network 117 and a portion of a static piece of information available to the mobile handset 107. The mobile handset 107 may comprise a management client 109, device wrappers 115, a transport client 111, and a device reader 113. The carrier network 117 may comprise a management server 121 and a transport server 119. In an embodiment of the present invention, the carrier network 117 may also comprise a provisioning system 123 and a billing system 125.

[0019] In an embodiment of the present invention, the manufacturer may provide the static piece of information available to the mobile handset 107. In such an embodiment, a wrapper provided as part of the device wrappers 115 may extract the static key. In another embodiment of the present invention, a carrier network may provide the static piece of information to the mobile handset 107 during a provisioning event of the mobile handset 107. In yet another embodiment of the present invention, a vendor whose software is installed on the mobile handset 107 may provide the static piece of information available to the mobile handset 107. In still another embodiment of the present invention, a management client 109 component of the mobile handset 107 may provide the static piece of information available to the mobile handset 107. In a further embodiment of the present invention, a Subscriber Identity Module (SIM) card inserted into the mobile handset 107 may provide the static piece of information available to the mobile handset 107.

[0020] In an embodiment of the present invention, the piece of information dynamically sent to the mobile handset 107 by the carrier network 117 may be communicated over a Wireless Application Protocol (WAP). In another embodiment of the present invention, the piece of information dynamically sent to the mobile handset 107 by the carrier network 117 may be communicated over a Short Message Service (SMS). In yet another embodiment of the present invention, the piece of information dynamically sent to the mobile handset 107 by the carrier network 117 may be communicated over a proprietary protocol.

[0021] The static piece of information may be a static key employed for security operations. The information dynamically sent to the mobile handset 107 may be a dynamic key, which may be combined with the static key to generate an encryption key, or a key for generating a hash code, etc.

[0022] In an embodiment of the present invention, the management client 109 may provide a secure storage and execution environment by employing a dynamic key and a static key for security, authentication, confidentiality, etc. The dynamic key may be either retrieved by the management client 109 from the management server 121 or sent to the management client 109 by the management server 121. In an embodiment of the present invention, the management server 121 may be capable of generating the dynamic keys based on user profile, device profile, device configuration and capabilities, update package availability, etc.

[0023] In an embodiment of the present invention, the management server 121 may determine whether the mobile handset 107 requires an update package. The management server 121 may also retrieve an address for the mobile handset 107 from the provisioning system 123, and generate a dynamic key for the mobile handset 107 based on a user profile retrieved from the provisioning system 123. The management server 121 may also assemble a notification message that contains the dynamic key, to be sent to the mobile handset 107, and instruct the transport server 119 to communicate the notification message to the mobile handset 107, and to subsequently process messages and/or requests sent to it by the mobile handset 107. These processed messages and/or requests may employ the dynamic key for security and/or authentication.

[0024] In an embodiment of the present invention, the management server 121, via the transport server 119, may send a dynamic key to the mobile handset 107 with a notification. The notification may, for example, inform a user about the availability of an update package. The management server 121 may encrypt the dynamic key by employing another key such as, for example, a content encryption key. The mobile handset 107 can decrypt the dynamic key using the same (in the case of symmetric keys) or a different (asymmetric keys) content encryption key. Only the management server 121 and the management client 109 in the mobile handset 107 may know the dynamic key. In an embodiment of the present invention, the dynamic key may be used in conjunction with a static key, such as an Electronic Serial Number (ESN) embedded in a mobile device 107, and retrieved employing the device

wrappers 115. In an embodiment of the present invention, the dynamic key may also be used together with a number such as, for example, a device key retrieved by the device reader 113 from a SIM card or any similar card reader or device such as, for example, a smart card, an integrated circuit (IC) card, etc. In an embodiment of the present invention, the dynamic key may also be used with a handset key such as, for example, a static key or a device key embedded in the management client 109.

[0025] In an embodiment of the present invention, the static key may be a device key, which may be used to authenticate a mobile handset 107 to the carrier network 117. A user may be associated with the device key, and by extension, with the mobile handset 107. Other identifications may be employed in place of the device key by the carrier network 117. The combination of the static key of the mobile handset 107 and the dynamic key managed by the management client 109 provides a user with better security over prior art solutions. It is very difficult for a third party such as, for example, a “hacker” to capture both the static key as well as the dynamic key(s) to illegally access data communicated between the mobile handset 107 and the carrier network 117. The use of the static key and the dynamic key together greatly reduces the likelihood that a third party is able to capture the pieces required to compromise security.

[0026] In an embodiment of the present invention, the static key may be a system key that may be also used by the carrier network 117 to authenticate system data, such as firmware updates sent to the mobile handset device 107 from the management server 121. In an embodiment of the present invention, only the management client 109 may be capable of accessing static keys such as, for example, the device key and the system key. In such an embodiment, the management client 109 may not be able to manipulate or modify the device key and the system key. In another embodiment of the present invention, only the management client 109 may be capable of accessing and/or modifying the device key and the system key.

[0027] In an embodiment of the present invention, the combination of the device key and the system key may be used as a device-independent key at the application level. In such an embodiment, the key combination may be useful for generating digital signatures on data communicated between the mobile handset 107 and the carrier network 117.

[0028] In an embodiment of the present invention, the dynamic key received by the mobile handset 107 may be combined with a static key, which may be available at the mobile handset 107, to generate a private key. The generated private key may then be employed to secure communications with the management server 121. The corresponding public key belonging to the management server 121 may have been provided to the mobile handset 107, for example, during a provisioning process, as part of a default configuration. The mobile handset 107 may then retrieve the dynamic key and a static key to generate the private key. The mobile handset 107 may employ the generated private key to read data sent to the mobile handset 107 by the management server 121. The mobile handset 107 may also employ the public key of the management server 121 for securing data communicated to the management server 121.

[0029] In an embodiment of the present invention, the device wrappers 115 may provide access to device-specific information, device configuration information, data, etc., in the mobile handset 107. In an embodiment of the present invention, the device wrappers 115 may provide access to a device key that is managed by the mobile handset 107, the device key having been stored in the non-volatile memory of the mobile handset 107. In a related embodiment of the present invention, the device key may be a key provided by the manufacturer of the mobile handset 107. In yet another embodiment of the present invention, the device wrappers 115 may provide access to a device key that is managed by the management client 109 of the mobile handset 107. In such an embodiment, the device key may be provided by the vendor of the management client 109 and installed in the non-volatile memory of the mobile handset 107 when the management client 109 is installed into the mobile handset 107.. In still another embodiment of the present invention, the device key may be provided to the mobile handset 107 when the mobile handset 107 is provisioned by the provisioning system 123.

[0030] In an embodiment of the present invention, the carrier network 117 may send a notification message to the mobile handset 107 via the transport server 119. The management server 121 may create the notification message to inform the user of the mobile handset 107 of an event such as, for example, the availability of a new update package for the mobile handset 107. The update package may be employed to update the firmware or software in the mobile handset 107. The management server 121 may contain a dynamic key

with the notification message for its retrieval by the mobile handset 107. The mobile handset 107 may receive the notification message via the transport client 111, process the notification message, retrieve the dynamic key sent with the notification message or embedded in the notification message, and store the dynamic key for subsequent usage. The received dynamic key may be subsequently employed by the management client 109 of the mobile handset 107 to retrieve update packages, configuration data, etc. from the management server 121. The received dynamic key may be combined with a static key retrieved from the mobile handset 107 (using device wrappers 115, for example) to encode requests for data sent to the management server 121, to authenticate data sent by the management server 121, to create a digital signature that accompanies any communication sent to the management server 121, to decode data received from the management server 121, etc. The dynamic key may be employed for all subsequent data communication until a new dynamic key is delivered by the management server 121 to the mobile handset 107, until a preset time period expires, or until a preset number of activities such as, for example, firmware downloads, configuration updates, data downloads, etc., take place.

[0031] In an embodiment of the present invention, the transport server 119 may be a Wireless Application Protocol- (WAP) compliant gateway. The transport client 111 may be a WAP-based client that can communicate with a WAP server such as, for example, the transport server 119. The management client 109 may be capable of monitoring and parsing Wireless Markup Language (WML) data received from the management server 121, and retrieving any keys accompanying commands communicated to the management client 109 by the management server 121. The management client 109 may save the received keys and/or commands for subsequent processing. If the management client 109 determines that WML (or eXtensible Markup Language (XML)) content received from the management server contains a dynamic key, the management client 109 may save the dynamic key in non-volatile memory and employ it during later communications with the management server.

[0032] In an embodiment of the present invention, the transport server 119 may be incorporated into the management server 121. In another embodiment of the present invention, the transport client 111 may be incorporated into the management client 109.

[0033] Fig. 1B illustrates a block diagram of an exemplary security system 155 for communicating data between a mobile handset and a management server, in accordance with

an embodiment of the present invention. The security system 155 may facilitate secure communication of data/code between a mobile handset 157 and a carrier network 167. The mobile handset 155 may comprise a management client 159, device wrappers 165, and a SMS client 161. In an embodiment of the present invention, the mobile handset 155 may also comprise a SIM card reader 163. The carrier network 167 may comprise a management server 171, and a SMS server 169. In an embodiment of the present invention, the carrier network 167 may also comprise a provisioning system 173 and a billing system 175.

[0034] In an embodiment of the present invention, the SMS server 169 may send a dynamic key to mobile handset 157 with a SMS (or other) notification, which may, for example, notify a user about the availability of an update package. The management server 121 may employ a content encryption key to encrypt the dynamic key. The mobile handset 157 may be capable of decrypting the dynamic key using the same content encryption key (in the case of symmetric keys) or using a different content encryption key (in the case of asymmetric keys). Only the carrier network 167 and the mobile handset 157 may know the dynamic key. The dynamic key may be used together with a static key such as, for example, an ESN contained in a mobile device, to provide for secure communications. In an embodiment of the present invention, the static key may be a number retrieved from a SIM card. In another embodiment of the present invention, the static key may be a mobile handset key embedded in the management client 159. In yet another embodiment of the present invention, the static key may be provided by the manufacturer, and may be extracted by a wrapper provided by the device wrappers 165. In a further embodiment of the present invention, a SIM card may provide the static key. In still another embodiment of the present invention, the management client 159 may provide the static key.

[0035] Fig. 2 illustrates a block diagram of an exemplary mobile handset 205 employing a management client 223 to manage secure communications of data/code with external systems such as a carrier network, in accordance with an embodiment of the present invention. The mobile handset 205 may comprise a management client 223, a transport client 227, applications 229, device configuration information 213, and device wrappers 219. In an embodiment of the present invention, the mobile handset 205 may further comprise a SIM card 209 and a SIM card reader 211. The management client 223 may comprise an upload agent 217, a download agent 215, a SMS Message Processor 221, and a security manager

225. In an embodiment of the present invention, the management client 223 may further comprise static key information 207.

[0036] The security manager 225 may be employed to facilitate secure communications based on encoding, encryption, authentication, etc. The security manager 225 allows accessing and storing static key information 207 that may be provided by the manufacturer at manufacturing time, or by a carrier during service provisioning. The security manager 225 may also support management of the life cycle of the static key information 207. In an embodiment of the present invention, the security manager 225 may facilitate accessing (via the SIM card reader 211) and manipulating security-related information provided by the SIM card 209. The security manager 225 may support retrieval and storage of dynamic keys communicated to the mobile handset 205 by external systems such as, for example, a carrier network. Such dynamic keys may be embedded in or enclosed within messages and/or notifications sent to the mobile handset 205 by the external systems. The security manager 225 may also be employed to encrypt/decrypt data that is sent to/received from the external systems. The security manager 225 may create message digests, digital signatures, etc. In an embodiment of the present invention, the security manager 225 may support public-key/private-key-based encryption/decryption. In such an embodiment, the security manager 225 may access the public key of external systems such as, for example, the management server of a carrier network. The public key may be then stored locally. In another embodiment of the present invention, the security manager 225 may also facilitate the modification and life cycle management of such public-keys.

[0037] In an embodiment of the present invention, the security manager 225 may utilize the SMS message processor 221 to monitor and process incoming SMS messages to retrieve dynamic keys. The dynamic keys may be sent with messages, notification, and/or data, which may be sent by an external system such as, for example, a carrier network.

[0038] In an embodiment of the present invention, the upload agent 217 may be employed to apply firmware/software updates retrieved from an external system. The device configuration information 213 may comprise device configurations such as addresses of RAM, ROM, FLASH, the sizes of volatile and non-volatile memory, etc. The download agent 215 may be used to download update packages for firmware/software. The transport client 227 may be employed to facilitate downloads performed by the download agent 215.

[0039] Fig. 3 illustrates a flow diagram 305 of an exemplary method of operating a secure system for communicating data between a mobile handset and a management server, in accordance with an embodiment of the present invention. At a start block 307, the user may acquire the mobile handset, and the carrier network may provision the handset for service. Then, at block 309, the mobile handset may be provisioned with a local key component such as a static key. In an embodiment of the present invention, the static key may be a device key. In another embodiment of present invention, the local key may be a system key. In another embodiment of present invention, the local key component may be a set of a device key and a system key. Other sets of keys may also be contemplated.

[0040] A SMS message may contain the dynamic key associated with the mobile handset. The SMS message with the dynamic key may be sent, at block 311, by the management server of a carrier network via a SMS server used as a transport server. In an embodiment of the present invention, the dynamic key may be sent as part of the text section of a SMS message. In such an embodiment, the dynamic key is included in the SMS message and the mobile handset parses the received message, and retrieves the dynamic key if one is included. In another embodiment of the present invention, the dynamic key may be attached as part of the data of a SMS message and the mobile handset can retrieve data (such as the dynamic key) associated with received SMS messages. The mobile handset may process SMS messages at block 313. Then, at block 315, the mobile handset may determine the dynamic key by parsing the SMS message and retrieving the dynamic key for subsequent usage. In an embodiment of the present invention, the mobile handset may also store the dynamic key in non-volatile memory such as FLASH.

[0041] The mobile handset may then retrieve the static key employing device wrappers, and generate a security key, at a block 317. In an embodiment of the present invention, the security key may be generated by concatenating the static key and the dynamic key. In another embodiment of the present invention, the security key may be combined with the dynamic key employing a key generation function.

[0042] Next, at block 319, the mobile handset may employ the security key to communicate with the management server, and send and receive data/code. In an embodiment of the present invention, the mobile handset may use the security key as a symmetric private key to encrypt data that is communicated to the management server of a carrier network. The

management server may then generate and employ the same security key to decrypt data sent to it by the mobile handset. In another embodiment of the present invention, the mobile handset may use the security key as a private key, and may decrypt data sent to it by the management server of a carrier network. In yet another embodiment of the present invention, the mobile handset may employ a public key of the management server. The public key may be retrieved employing device wrappers or SIM cards, and used to encrypt data sent to the management server. In another embodiment of the present invention, the public key may be retrieved from non-volatile memory.

[0043] The management server of the carrier network may, at block 321, verify the access from the mobile handset by performing a security check. In an embodiment of the present invention, the security check may involve decrypting the received data/ message/ request by using a private key and ensuring that the received data/ message/ request is valid and authorized. Other forms of security checks may be also utilized. In an embodiment of the present invention, symmetric key generation and validation of data sent by the mobile handset may also be employed.

[0044] A user may utilize the mobile handset to request update packages, and the request may be processed and update packages and/ or data may be provided to an authorized user at block 323. The processing for communicating data may then be completed at block 325.

[0045] In an embodiment of the present invention, Internet Over The Air (IOTA) and Synchronization Markup Language- (SyncML) based data transport mechanisms may be employed to communicate the dynamic key (or encoded/encrypted versions of one or more dynamic keys) from the server-side to the client side. The client-side may monitor data provided by the server-side to determine whether dynamic key(s) are included in the data. If a dynamic key(s) is determined to exist in the data, it may be retrieved and stored for subsequent access/usage.

[0046] In an embodiment of the present invention, the life cycle of dynamic keys may be managed by the mobile handset. An expiration date may be specified/provided along with the dynamic key(s). If an expiration date is not specified, a default expiration date for the dynamic key(s) may be supplied by the mobile handset.

[0047] In an embodiment of the present invention, the dynamic key may be employed to create a symmetric key in the mobile handset. In such an embodiment, other information

may also be employed along with the dynamic key, to create the symmetric key in the mobile handset. In another embodiment of the present invention, the dynamic key may be employed to create a private key in the mobile handset. In such an embodiment, other information may be also employed along with the dynamic key to create the private key in the mobile handset. In such an embodiment, a public key corresponding to the private key may be available from the mobile handset. Other security-related uses for the dynamic key are also contemplated.

[0048] While the present invention has been described with reference to certain embodiments, it will be understood by those skilled in the art that various changes may be made and equivalents may be substituted without departing from the scope of the present invention. In addition, many modifications may be made to adapt a particular situation or material to the teachings of the present invention without departing from its scope. Therefore, it is intended that the present invention not be limited to the particular embodiment disclosed, but that the present invention will include all embodiments falling within the scope of the appended claims.